

(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 1)

(11)特許番号

第2884338号

(45)発行日 平成11年(1999) 4月19日

(24)登録日 平成11年(1999) 2月12日

(51)Int.Cl.⁸

識別記号

F I

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 D

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 C

15/00

3 3 0

15/00

3 3 0 B

H 0 4 L 9/00

6 7 3 D

発明の数 2 (全 14 頁)

(21)出願番号

特願平9-264850

(62)分割の表示

特願平8-56966の分割

(22)出願日

昭和59年(1984)10月11日

審査請求日

平成9年(1997)10月13日

許権者において、権利譲渡または実施許諾の用意がある。

早期審査対象出願

(73)特許権者 593187342

塚本 豊

奈良県吉野郡大淀町大字北野40番地の15

(72)発明者

塚本 豊

岡山県玉野市玉4丁目8番20号

審査官 徳永 民雄

(56)参考文献

特開 昭52-59540 (J P, A)

特開 昭57-111760 (J P, A)

(58)調査した分野(Int.Cl.⁸, D B名)

H04L 9/00 - 9/38

H04K 1/00 - 3/00

G09C 1/00 - 5/00

G06F 15/00

G06F 12/00

(54)【発明の名称】 アクセス制御システム

1

(57)【特許請求の範囲】

1. アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、

前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なう集中管理を行なう認証手段と、

演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化する可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含む、

2

前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、

前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、

前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、

前記アクセス制御システムは、

前記可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を

10

3

自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段をさらに含み、

前記アクセス希望者は、前記認証手段により適正である旨の認証結果が得られたことを条件として前記アクセス対象へのアクセスが許容されることを特徴とする、アクセス制御システム。

2. アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、

前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、

演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化する可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、

前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、

前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、

前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして利用して前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、

前記時間同期式認証手段は、前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段と、

前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段とを含むことを特徴とする、アクセス制御システム。

3. 前記可変型パスワードデータ生成手段は、当該可変型パスワードデータ生成手段を所有している本人を確認するための識別データ信号が入力されたことを判別する識別信号入力判別手段を含み、該識別信号入力判別手段による入力判別が行なわれたことを条件として前記可変型パスワードデータの生成が可能となることを特徴とす

4

る、請求項1または請求項2に記載のアクセス制御システム。

4. 前記認証手段が前記可変型パスワードデータに基づいたパスワード認証動作を行なう前に、前記アクセス希望者から通知された確認用データであって当該アクセス希望者が予め登録されているものか否かを確認するための登録確認用データに基づいて適正である旨の確認結果が得られたことを条件として、前記認証手段が前記パスワード認証動作を実行することを特徴とする、請求項1または請求項2に記載のアクセス制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、主として、あるアクセス対象設備へのアクセスを限られた者にのみ限定するべく、アクセス対象設備へのアクセスが許されるべきものか否かを認証してアクセス制御を行なうアクセス制御システムであり、詳しくは、アクセス希望者側がパスワードデータをデータ通信により伝送し、その伝送されてきたパスワードデータに基づいてアクセス制御を行なうアクセス制御システムに関する。

【0002】

【従来の技術】この種のアクセス制御システムにおいて、従来から一般的に知られているものに、たとえば、特開昭59-10680号公報に記載のものがあつた。この従来技術のものは、アクセス対象設備に一定のシークレットルール（パスワードデータの適否を判定する判定用データ）を前もって登録しておき、アクセス対象設備側で生成された乱数がアクセス希望者所有のパスワードデータ生成装置に入力されてその乱数を用いて生成されたパスワードデータが前記アクセス対象設備側に伝送され、前記アクセス対象設備側で前記登録されていたシークレットルールを用いて生成されたパスワードデータと伝送されてきたパスワードとが一致する場合にのみ、アクセス希望者が適正である旨の判別を行なってアクセス対象設備へのアクセスを許容するように構成されていた。つまり、前記乱数により、アクセス毎に変化可能なデータであってアクセス希望者側とアクセス対象設備側とで共通に変化可能な共通変化データが構成されており、この共通変化データを利用して毎回変化するパスワードデータを生成してアクセス可否の認証を行なっていた。

【0003】ところが、高度情報化社会となり、この種のアクセス制御システムが普及した場合には、たとえば、コインロッカーのドアの解錠、自己の銀行口座の呼出し、使用者が限定されているシークレットな技術情報のファイル装置等からの呼出し等、本システムの使用頻度が増大し、多くのアクセス対象設備へのアクセスに使用されることになる。その結果、ユーザが利用しようとする多くのアクセス対象設備すべてに逐一前記シークレットルール等の判定用データを登録しておかなければな

5

らず、それだけ登録された判定用データの他人による盗用の機会が増大し、悪用による多大な損害が発生するという欠点が生ずる。特に高度情報化社会においては、個人のプライバシーや企業秘密の漏洩は万が一にもあってはならないのであり、前述した判定用データの盗用は厳に防止しなければならない。

【0004】

【発明が解決しようとする課題】そこで、アクセス対象設備毎に異なった判定用データを登録し、たとえばそのうちの1つの判定用データが盗まれたとしても、他のアクセス対象設備へのアクセスに悪用されないようにする方法も考えられる。しかし、アクセス対象設備毎に使用対象となる判定用データをユーザが記憶または所有しておかなければならず、煩雑であり、特に、アクセス対象設備が多くなれば忘れる可能性もあり、不都合である。

【0005】また、仮りに、前記登録された判定用データの盗用を完全に防止できたとしても、多くのアクセス対象設備すべてに逐一前記判定用データを登録するという従来技術の場合には、多くのアクセス対象設備に逐一判定用データを登録するという煩雑な作業が必要となるばかりでなく、たとえば前記パスワードデータ生成装置が盗難される等の原因で前記判定用データを新たなものに更新しなければならなくなった場合には、多くのアクセス対象設備すべてに登録されている判定用データを逐一すべて更新し直さなければならず、非常に煩雑な作業が強いられるという欠点が生ずる。本発明は、係る実情に鑑み考え出されたものであり、その目的は、アクセス対象が多くなったとしても、その多くのアクセス対象毎に判定用データの登録を行なう必要性をなくして、アクセス対象毎に判定用データの登録を行なうことによる前述した種々の不都合を防止できるアクセス制御システムを提供することである。

【0006】

【課題を解決するための手段】本第1発明は、アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、前記可

6

変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、前記アクセス制御システムは、前記可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることを防止可能とするための誤差自動修復手段をさらに含み、前記アクセス希望者は、前記認証手段により適正である旨の認証結果が得られたことを条件として前記アクセス対象へのアクセスが許容されることを特徴とする。本第2発明は、アクセス希望者側が生成したパスワードデータに基づいて認証を行ないアクセス制御を行なうためのアクセス制御システムであって、前記アクセス希望者がアクセスしようとする対象であって複数箇所に分散配置された複数のアクセス対象と、該複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証を統括して行なって集中管理を行なう認証手段と、演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する手段であって、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化可能な可変型パスワードデータを演算して生成する可変型パスワードデータ生成手段とを含み、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを伝送した場合に該可変型パスワードデータが前記認証手段に転送され、前記可変型パスワードデータ生成手段は、クロック機能を有し、該クロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータを生成し、前記認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして利用して前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含み、前記時間同期式認証手段は、前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段と、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段とを含むことを特徴とする。

【0007】

【作用】本第1発明によれば、複数箇所に分散配置された複数のアクセス対象に対し統括して認証を行なう認証手段が設置されており、その認証手段により、前記複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証が統括して行なわれて集中管理が行なわれる。演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する可変型パスワードデータ生成手段の働きにより、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化する可変型パスワードデータが演算されて生成される。そして、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを転送した場合にその可変型パスワードデータが前記認証手段に転送される。前記可変型パスワードデータ生成手段は、クロック機能を有しており、そのクロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータが生成される。認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段を含んでいる。そして、誤差自動修復手段の働きにより、可変型パスワードデータ生成手段のクロックが狂って前記時間変数データに誤差が生じた場合にその誤差を自動的に修復させて経時的に誤差が累積されることが防止可能となる。そして、アクセス希望者は、認証手段により適正である旨の認証結果が得られたことを条件としてアクセス対象へのアクセスが許容される。本第2発明によれば、複数箇所に分散配置された複数のアクセス対象に対し統括して認証を行なう認証手段が設置されており、その認証手段により、前記複数のアクセス対象それぞれについてアクセス要求があった場合のアクセス制御のための認証が統括して行なわれて集中管理が行なわれる。演算処理機能を有して前記アクセス希望者側においてパスワードデータを生成する可変型パスワードデータ生成手段の働きにより、前記アクセス希望者側と前記認証手段側とでアクセス毎に共通に変化可能な共通変化データを利用してアクセス毎に内容が変化する可変型パスワードデータが演算されて生成される。そして、前記アクセス希望者側が前記複数のアクセス対象のいずれかにアクセスするべく前記可変型パスワードデータを転送した場合にその可変型パスワードデータが前記認証手段に転送される。前記可変型パスワードデータ生成手段は、クロック機能を有しており、そのクロック機能が計時する時間に応じて変化する時間変数データを前記共通変化データとして利用して前記可変型パスワードデータが生成される。認証手段は、時間に応じて変化する時間変数データを前記共通変化データとして用いて前記転送されてきた可変型パスワードデータの適否を判定して認証を行な

う時間同期式認証手段を含んでいる。そして、所定誤差許容認証手段の働きにより、前記転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証が行なわれない。また、誤差許容時間内不正アクセス禁止手段の働きにより、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定が行なわれる。

【0008】

【発明の実施の形態】本発明に係るアクセス制御システムの実施の形態を説明する前に、高度情報化社会におけるデータ通信では必要性が高まるデジタル署名システムの実施の形態について説明する。

【0009】図1に示すように、文字用キーと数字用キーにより平仮名と数字をインプットできるキーボード1を有するデータ入力手段の一例のデータ入力装置2に対し、RAMやCPU内蔵のパーソナル端末装置3を着脱自在に構成している。このパーソナル端末装置はデジタル署名をせんとするデータの送信者が個人的に所有する装置であればどのようなものであってもよく、従来から一般的に周知なものとしては、たとえばICカード等が考えられる。

【0010】この個人所有のパーソナル端末装置3の回路構成を図10に示す。パーソナル端末装置3内には、CPU50と、ROM51と、RAM52と、I/Oポート53とが設けられている。ROM51は、CPU50の動作プログラムすなわち後述する図2に示すフローチャートのプログラム等が記憶されている。CPU50は、そのROM51に記憶されているプログラムに従って動作し、後述する秘密ルールの一例の文字数字変換ルールやシークレット関数を呼出してRAM52に記憶させる。そして、後述するように、キーボード1から入力されてI/Oポート53から入力された送信データを、RAM52に記憶されている秘密ルールに従ったアルゴリズムにより、図2に示すように変換し、その変換データをI/Oポート53から出力する。

【0011】このパーソナル端末装置3に記憶されている秘密ルールは、平仮名字を一定のルールに従って数字に変換するための文字数字変換ルールと、三角関数、指数関数等の組合せからなるシークレット関数 $f(x)$ 等から構成されている。この秘密ルールはパーソナル端末装置3においてそれぞれ相違した種類のものが記憶され、そのため、署名せんとする各署名者がそれぞれこのパーソナル端末装置3を所有することによって、各署名者はそれぞれ自己固有の秘密ルールを保有することになる。また、この秘密ルールは対外的に秘密なものであ

る。

【0012】そして、前記パーソナル端末装置3には、図2に示すフローチャートのプログラムが組込まれており、デジタル署名を行なう場合には、前記パーソナル端末装置3を入力装置2に装着した状態で署名対象である契約書の文字等の送信データを平仮名の形でキーボード1から入力する。また、日付等の数字はそのまま入力する。そして、入力されたものが文字である場合には、前記文字数字変換ルールに従って入力毎に逐一文字を数字に変換して足し合わせ、さらに、入力されたものが数字である場合には、その数字をそのままの形で足し合わせ、次にEND用キーEのON操作があれば、すべての文字、数字の和 $P(n)$ を前記シークレット関数 f

(x)に代入して答を算出し、その暗号化された符号からなる答である変換データ（この場合は数字となる）を署名データとしてI/Oポート53から出力して表示部4に表示させる。そして、その表示部4に示された署名データを認証対象となる契約書等の送信データとともに送信する。

【0013】前記入力装置2は、テレテックス端末機であってもよく、その場合には、署名対象物である送信データをテレテックス端末機のキーボードからパーソナル端末装置3に入力する。また、パーソナル端末装置3から出力された変換データである認証データを契約相手にテレテックス端末機から伝送するよう構成する。

【0014】さらに、前記文字数字変換ルールとシークレット関数とからなる秘密ルールは、秘守義務のある官公庁等の公共機関やサービス機関等に登録しておく。

【0015】書類受付印、受理印、金銭領収印のように、チェックのための認証を行なうデジタル署名の場合には、書類受付行為等の認証対象行為自体を平仮名文字でキーボード1から入力し、さらに、認証対象行為を行なった日付を入力して変換データすなわち署名データを算出する。たとえば、認証対象行為が書類受付であり、認証日付が1984年10月9日11時35分であれば、キーボード1に、「しよるいうけつけ1984ねん10がつ9ひ11じ35ふん」と入力する。

【0016】また、書類受付行為、受理行為等の種々の代表的チェック行為をキーボード1における1つの操作ボタンに割り付けることによってワンタッチで入力できるように構成してもよい。

【0017】さらに、本発明でいう認証対象行為として挙げた書類受付行為、受理行為等は単なる例示であり、その他、注文書、納品書、領収書等への認証における注文行為、品物納入行為、金銭領収行為等、種々のチェック行為が含まれることは言うまでもない。

【0018】次に、別の例を説明する。

① シークレット関数によって算出された数字をそのまま署名データとする代わりに、その算出された数字の一部または全部を、一定のシークレットなルールに基づい

て、平仮名、片仮名、漢字アルファベット等の文字や、図形、記号またはそれらの組合せまたはそれらと色彩との組合せに変換して署名データとして用いる。

【0019】② 前記秘密ルールをパーソナル端末装置3に記憶させる代わりに、図3に示すように、企業等のファイル装置5に記憶させておく。その場合には、テレテックス端末機6と前記ファイル装置5とをコンピュータ7を介してLAN8等で接続し、公衆回線等を利用して他の企業との間で行なわれるペーパレス取引の署名者が、自己の秘密ルールを前記テレテックス端末機6からの操作で呼出し、前記コンピュータ7によって暗号化等の変換作業を行なう。前記秘密ルール呼出しの際には、後述する個体識別システムを利用して、署名者が呼出指定している秘密ルールが本当にその署名者のものであるか否かをコンピュータ7によりチェックし、署名者のものであることが確認できた段階で初めて呼出指定された秘密ルールへのアクセスを可能にする。

【0020】なお、図中9はノードである。

③ 秘密ルールを企業内のファイル装置5から呼出す代わりに、秘密ルールが登録されている公共機関やサービス機関等のファイル装置、または、自宅のファイル装置からデータ通信により自己の秘密ルールを呼出し、その呼出したファイル装置に接続されているコンピュータで暗号化等の変換作業を行なう。

【0021】④ 前記パーソナル端末装置3を、その装置所有者が所有する発信機（たとえば指輪型のもの）からの所定の信号（発信機それぞれによって相違する）を受信できなくなれば、暗号化等の変換機能が停止するように構成し、パーソナル端末装置3の紛失時における他人の悪用を防止できるようにする。

【0022】⑤ 暗号化等の変換方法として、図2に示した $P(N) = P(N-1) + D(N)$ の代わりに、 $P(N) = P(N-1) + N \cdot D(N)$ 、 $P(N) = P(N-1) + D(N) / N$ 、 $P(N) = P(N-1) / N + D(N)$ 、あるいは、 $P(N) = P(N-1) / N + N \cdot D(N)$ 等を用いる。

【0023】次に、本発明に係るアクセス制御システム（個体識別システム）の実施の形態について説明する。このアクセス制御システムは、たとえば、前述したように、秘密ルール読出の際に読出指定された秘密ルールが本当に本人のものであるか否かを判別する等の場合にも利用できる。

【0024】図4に示すように、銀行10内の自己の口座の呼出し、データバンク11内のシークレットな技術情報の検索、コインロッカ12の解錠等、一定の限られたものにのみアクセスを許容すべき設備と、設備利用者（アクセス希望者）にアクセスを許容してもよいか否かの個体識別を判断する自宅または所定の機関のコンピュータ13または14とを公衆回線15で接続し、それら設備10、11、12と個体識別を行なうコンピュー

10

20

30

40

50

タ13、14との間でデータ通信が可能になるように構成している。また図中16は網制御装置（NCU）、17は交換機である。

【0025】そして、たとえば、データバンク11内の技術情報を利用したい場合には、まず、キャプテン用端末機18により、データバンク11を呼出して所望の技術情報を検索してもらい、その技術情報が或る一定のものにしか使用許可されないシークレットな技術情報である場合には、以下の手順で個体識別を行なう。

【0026】① 技術情報を使用せんとする設備利用者が個体識別を行なう自宅または所定機関のコンピュータ13または14の呼出番号をデータバンク11に知らせる。

【0027】② データバンク11側は、その番号が前もって登録されている使用許可できるものの番号であるか否かを確認し、使用許可者の番号であれば識別信号の送信を要求し、使用許可者の番号でなければ使用を許可しない。

【0028】③ 前記識別信号の送信要求ができれば設備利用者は自己所有の装置33からアウトプットされた識別信号をキャプテン用端末機18によりデータバンク11側に送信する。

【0029】④ データバンク11側は送信されてきた識別信号を前記呼出番号のコンピュータ13または14に送信し、そのコンピュータ13または14で送信されてきた識別信号が正しいものか否かの個体識別判断（後述する）を行ない、その結果をデータバンク11側に送信する。

【0030】⑤ データバンク11側では、正しいという判断結果が送信されてきた場合にのみ呼出指定されているシークレット技術情報へのアクセスを許可する。

【0031】次に、コインロッカ12を解錠する場合の手順は、まず、解錠状態にあるコインロッカのドア内面側にあるキーボードの操作によって個体識別を行なう自宅または所定機関のコンピュータ13または14の呼出番号をインプットし、予め前記コンピュータ13または14を登録し解錠操作時に自動的にそのコンピュータ13または14が呼出されるように設定した状態でドアを閉じて錠をかけ、解錠時には、そのコインロッカのドア外面から識別信号をインプットし、前述した④、⑤と同様の方法により解錠制御を行なう。

【0032】次に、たとえば、金銭の支払いに際して、自己の銀行口座の預金を金銭受取人の銀行口座内に移動させるという数字の移動のみで現金の移動を伴わないキャッシュレス支払システム（銀行POSシステム）等において、自己の銀行口座を呼出す手順は、まず、銀行に前もって自宅または所定機関のコンピュータ13または14の呼出番号を登録しておき、自己の銀行口座の呼出指定があった場合には、自動的に前記コンピュータ13または14が呼出されるように設定しておく。そして、

スーパーマーケット等で物を購入して支払いをする場合には、そのスーパーマーケット等のレジスタ19から自己の銀行口座の呼出指定を行ない、前記④、⑤と同様の方法で自己の銀行口座へのアクセスを行なう。なお、自己の銀行口座呼出指定手段としては、設備利用者所有の装置33から出力された銀行口座呼出指定信号をレジスタ19から入力し、銀行へ伝送する方法を用いる。

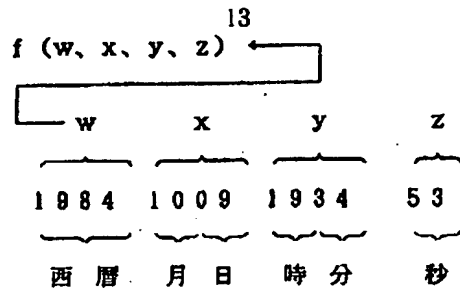
【0033】また、自動車等のドアの解錠、エンジンの始動等のアクセスは利用対象設備が移動物であるために、公衆回線等の有線系メディアによるデータ通信は不可能であり、衛星通信等の無線系メディアを用いる。このように、本発明でいう「データ通信」とは、有線系メディアばかりでなく無線系メディアをも含む広い概念である。

【0034】次に、前述した個体識別方法を説明する。図5に示すように、JJYによる時刻標準電波等のコード／データ放送を受信し、その受信信号に基づいて時刻を表示する腕時計により設備利用者所有の装置33を構成してある。そして、腕時計33内に記憶されているシークレットルールとしてのシークレット関数（それぞれの腕時計によって相違する）に、その腕時計33が表示している現在の時刻を入力信号として代入し、答えを算出し、その答えと使用した入力信号のうち秒に相当する部分を識別信号としてアウトプットする。アウトプットの方法は、図6に示すように、まず送信ボタン21を押し、腕時計裏面の伝導板からなる信号送出し部22から手23にパルス電流として識別信号が一定時間（10秒間）送り出され、導体である手23を媒体として、レジスタ19、コインロッカ12、自動車20、キャプテン用端末機18、電話機、テレックス用端末機等の識別信号受信部24へ送信される。送信された識別信号は、個体識別判断を行なう自宅または所定の機関のコンピュータ13または14へ送られ、そのコンピュータに予め登録されているシークレットルールとしてのシークレット関数に入力信号を代入して答えを算出し、その答えと識別信号とを比較して正しいか否かを判断し、個体識別を行なう。

【0035】前記シークレット関数は、三角関数、指数関数等の組合せからなる関数で、4つの変数w、x、y、zを有し、以下に示す数1のように、入力信号のそれぞれの部分をw、x、y、zに代入して答えを算出する。

【0036】

【数1】



【0037】また、外国から我が国へ識別信号を送る場合には、外国の時刻を我が国の時刻に変換した入力信号をシークレット関数に代入する必要がある。

【0038】図中25は或る一定の信号を発生する設備利用者所有の指輪型発信機であり、発信機それぞれによって発信信号が相違するもので、前記腕時計33が、その発信機25からの所定の信号を受信しているときにのみ識別信号を発信するように構成し、腕時計33紛失時における他人の悪用を防止する。

【0039】図中26は、自己の銀行口座呼出しの際等に使用するキーボードであり、暗証番号をインプットしたり、銀行口座呼出指定信号をアウトプットさせたりするもので、それら信号は、識別信号と同様に信号送出し部22からアウトプットされる。

【0040】なお、前記腕時計33は、コード/データ放送による信号に基づいて逐一表示時刻との誤差が修正されるように構成されているものであり、腕時計33内に組込まれるプログラムのフローチャートを図7に示す。ゆえに、この腕時計33は、プログラムに従って動作するマイクロコンピュータすなわち図10に示す回路構成と同様のものが内蔵されている。

【0041】図7に示すフローチャートを簡単に説明する。ステップS（以下単にSという）1により、コード/データ放送による時刻標準電波を受信したか否か判断され、受信するまで待機する。そして受信した場合にはS2に進み、その時刻標準電波に基づき分周器を修正し、修正後の時刻を表示する動作が行なわれる。次にS3に進み、受信機25（図5参照）からの信号を受信しているか否かの判断がなされ、受信していない場合にはS1に戻るが、受信している場合にはS4に進み、個人識別信号の受信ボタン21（図6参照）がON操作されたか否かの判断がなされ、操作されていない場合にはS1に戻るが、操作された場合にはS5に進み、シークレット関数 $f(w, x, y, z)$ のそれぞれの w, x, y, z に現在の時刻からなる入力信号を代入し、答えAを算出する処理がなされる。次にS6に進み、その算出した答えAと z に代入された数値NZとを識別信号としてアウトプットする処理がなされる。

【0042】次に、シークレットルールが登録されているコンピュータ13または14に組込まれるプログラムのフローチャートを図8に示す。図8に基づいてこのフ

14

ローチャートを簡単に説明する。S7において、識別信号AとNZとを受信したか否かの判断がなされ、受信するまで待機する。そして受信した段階でS8に進み、現在の時刻とNZとの差が許容値K秒以内であるか否かの判断がなされ、許容値K秒以内でなかった場合には、S12に進み、設備へのアクセスは許容できないとの判断をアウトプットする処理がなされてS7に戻る。この許容値Kは、腕時計33内で識別信号を算出するまでに要する時間やシークレットルール登録コンピュータ13または14までのデータ通信所要時間等を考慮した遅延時間であり、たとえば3秒等の短い時間である。

【0043】そして、S8により許容値K秒以内であると判断された場合にはS9に進み、今回の識別信号受信時刻が前回の受信時刻から前記許容値K秒以上経過しているか否かの判断がなされ、経過していない場合にはS12に進み、アクセスが許容できない旨の判断がなされる。このように、今回の識別信号受信時刻が前回の識別信号受信時刻から前記許容値K秒以上経過していることがアクセス許容条件に加えられている理由は、識別信号Aと前記NZが送信されたときから前記許容値K秒以内においてシステム悪用者が前記識別信号Aと前記NZとを記録してシークレットルール登録コンピュータ13または14に送信して不当に設備へのアクセスを行なう不都合を防止するためである。

【0044】そしてこのS9により許容値K秒以上経過していると判断された場合にはS10に進み、予め登録されているシークレット関数 $f(w, x, y, z)$ の w, x, y に現在の時刻からなる入力信号を代入し、 z に前記NZを代入して答えBを算出する処理がなされる。そしてS11に進み、そのBと前記受信したAとが等しいか否かの判断がなされ、等しくなければS12に進み、アクセスを許容できない旨の判断がなされ、等しい場合にはS13に進み、設備へのアクセスを許容できるとの判断をアウトプットする処理がなされてS7に戻る。

【0045】次に、この固体識別システムの発明の別実施の形態を説明する。

(1) 前記シークレット関数への入力信号として、現在の時刻を用いる代わりに、コード/データ放送に基づいて経時的に増加または減少する全国共通または全世界共通の数字を用いる。その場合に、レジスタ19、キャプテン用端末機18等の識別信号入力端子から前記入力信号用数字を発信してもよく、設備利用者所有の装置33への送信手段は、電波送信またはケーブルの接続のどちらでもよい。

【0046】さらに、設備利用者所有の装置33は腕時計に限らず、電子卓上計算機等の個人端末であれば何でもよい。

【0047】(2) 入力信号として、未だに使用されたことのないものを用いる選択使用手段として、過去に

10

20

30

40

50

用いられたことのある入力信号を拒絶する機能をシークレットルール登録コンピュータ13または14に付加する。この場合のシークレットルール登録コンピュータ13または14に組込むプログラム、設備利用者所有の装置33に組込むプログラムのそれぞれのフローチャートを図9(A)、(B)に示す。

【0048】この図9(A)、(B)に示すフローチャートを簡単に説明する。まず図9(B)に基づいて設備利用者所有の装置33に組込まれているプログラムを説明する。S22において、Iの初期値が「1」に設定される。次にS23に進み、送信ボタン21(図6参照)がON操作されたか否かの判断がなされ、されるまで待機する。そして操作された段階でS24に進み、シークレット関数 $f(x)$ に前記Iを代入し、 $f(I)$ の値Aを算出する処理がなされる。この段階では、前記Iは「1」となっている。次にS25に進み、A、Iそれぞれの値を識別信号としてアウトプットする処理がなされ、次にS26に進み、現在のIの値に「1」を加算して新たなIの値とする処理がなされた後にS23に戻る。

【0049】このように、設備利用者所有の装置33を利用して第1回目のアクセスを試みる場合には、前記 $f(I)$ に $I=1$ が代入されて算出された識別信号Aがシークレットルール登録コンピュータ13または14に伝送されることとなる。そして2回目のアクセスを試みる場合には、設備利用者所有の装置33の送信ボタン21がON操作されてS24の識別信号Aを算出する段階では、 $I=2$ となっているために、 $f(I)$ に $I=2$ が代入されて算出された識別信号Aが伝送されることとなる。

【0050】このように、装置33では、送信ボタン21がON送信されてアクセス動作が行なわれるたびにIが「1」ずつ加算更新されるために、アクセス動作するたびに毎回異なったIが用いられ、その結果毎回異なった識別信号Aが算出されて伝送されることとなる。

【0051】次にシークレットルール登録コンピュータ13または14に組込まれているプログラムを図9

(A)に基づいて説明する。S14により、Jの初期値が「1」に設定され、次にS15に進み、装置33から伝送されてきた識別信号IとAとを受信したか否かの判断がなされ、受信するまで待機する。そして受信した段階でS16に進み、 $J=I$ であるか否かの判断がなされる。第1回目のアクセス動作時においては、Jが「1」となっており、Iも「1」となっているはずであるために、S16によりYESの判断がなされるはずである。ところが、不正に設備へのアクセスを試みんとした者は、現時点でIがいくらの値になっているか判別できないために、Iに適当な値を代入してコンピュータ13または14に伝送する場合が考えられる。その場合には、S16によりNOの判断がなされてS17に進み、設備

へのアクセスを許容できないとの判断をアウトプットする処理がなされてS15に戻る。

【0052】一方、 $J=I$ と判断された場合にはS18に進み、登録されているシークレット関数 $f(x)$ にJを代入して答えBを算出する処理がなされる。次にS19に進み、その算出したBと前記伝送されてきたAとが等しいか否かの判断がなされ、等しくない場合にはS17に進み、設備へのアクセスを許容できない旨の判断がなされるが、等しい場合にはS20に進み、設備へのアクセスを許容できるとの判断をアウトプットする処理がなされる。次にS21に進み、現時点でのJの値に「1」を加算してJを更新する処理がなされた後S15に戻る。

【0053】このように、シークレットルール登録コンピュータ13または14は、装置33から識別信号A、Iが伝送されてくるたびにJの値を「1」ずつ加算更新するのであり、その結果装置33の現時点におけるIの値とシークレットルール登録コンピュータ13または14の現時点におけるJの値とは同期して同じ値となっているはずである。

【0054】(3) 指名手配者等の操作対象人間のシークレットルールを登録し、そのシークレットルール登録コンピュータに識別信号が伝送されてきた場合には、その識別信号を入力した端末機に場所通達指令信号を返送し、その端末機から警察のコンピュータ等に端末機設置場所を表示する信号を伝送するように構成する。

【0055】(4) 前記固体識別のために用いられたシークレットルールを前述のデジタル署名システムの発明に用いた秘密ルールによって肩代わりさせる。つまり、ある人物が所有する秘密ルールを、前記デジタル署名システムと固体識別システムとに兼用使用する。

【0056】次に、以上説明した種々の実施の形態の内容をまとめて以下に列挙する。

① 前記固体識別システム(アクセス制御システム)において、前記選択使用手段として、過去において使用されたことのある入力信号を拒絶する機能を前記判断手段側に持たせる。

【0057】② 前記固体識別システムにおいて、前記選択使用手段として、全国共通でしかも選択使用毎にまたは経時的に増加または減少する数字を前記入力信号として用いる。

【0058】③ 前記②に記載した固体識別システムにおいて、前記数字が、コード/データ放送によって伝送されてきた信号に基づいて定められたものである。

【0059】④ 前記②または③に記載された固体識別システムにおいて、前記数字が、現在の年月日時刻を表わすものである。

【0060】⑤ 前記②に記載された固体識別システムにおいて、前記設備利用者の装置が腕時計で構成され、その腕時計が表示されている時刻を入力信号として使用

する。

【0061】⑥ 前記⑤に記載した固体識別システムにおいて、前記腕時計が、コード／データ放送によって伝送されてきた信号に基づいて時刻表示可能なものである。

【0062】⑦ 前記③または⑥に記載の固体識別システムにおいて、前記コード／データ放送が、利用対象となる個々の設備から発信されているものである。

【0063】⑧ 前記⑤または⑥に記載の固体識別システムにおいて、前記腕時計が、アウトプットされた識別信号を人間の手を媒体として利用対象設備側に伝送するべく、人間の手への信号送り出し部を有するものである。

【0064】⑨ 前記固体識別システムにおいて、前記設備利用者所有の装置が、その装置所有者が所有する発信機からの所定の信号を受信できなくなれば、固体識別のための機能が停止するもので構成されている。

【0065】次に、本発明の構成要件と前記実施の形態との対応関係を説明する。前記シークレット関数 f

(w, x, y, z) または図9に示した $f(I), f(x)$ により、アクセス希望者固有の秘密の変換用データが構成されている。前記設備利用者所有の装置33により、アクセス希望者固有の秘密の変換用データを記憶している、前記アクセス希望者所有のパーソナル演算装置が構成されている。そして、前述したように、図7のS5、図8のS10に示された現在の時刻あるいは図9のS24に示されたI、S18に示されたJにより、前記パーソナル演算装置と後述するアクセス許否判定手段との両者に共通に使用される変数データであって、前回のアクセス時と今回のアクセス時とで変化する変数データが構成されている。そして前記パーソナル演算装置は、前述したように、前記秘密の変換用データに従って所定のアルゴリズムにより前記選択された変数データを変換するための動作機能を有する。

【0066】前記シークレットルール登録コンピュータ13または14により、アクセスを許容するか否かを判定するアクセス許否判定手段が構成されている。前記パーソナル演算装置が変換した変換済みデータ(A等の識別信号)は、前述したように、前記データ通信(図4参照)により前記アクセス許否判定手段に伝送される。そしてアクセス許否判定手段は、前記伝送されてきた変換済みデータの適否を前記選択された変数データに基づいて判別する。

【0067】前記銀行10、データバンク11またはコインロッカー12により、アクセス希望者がアクセスしようとするアクセス対象が構成されている。コンピュータ13または14により、前記アクセス対象とは別の場所に設置されて該アクセス対象側とデータ通信が可能であり、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段が構成されている。そして、前

述したように、アクセス希望者側が前記アクセス対象側に前記パスワードデータを伝送した場合にはそのパスワードデータがデータ通信により前記認証手段に転送される。

【0068】図8のS10のシークレット関数 $f(w, x, y, z)$ により、アクセス希望者側の前記パスワードデータの適否を判定するための判定用データが構成されている。そして前記認証手段は、前記アクセス希望者側の前記パスワードデータの適否を判定するための判定用データが格納されており、その判定用データを用いて前記転送されてきたパスワードデータの適否を判定して認証を行ない(図8のS11)、その認証結果を前記パスワードデータの転送元であるアクセス対象側に返信する。

【0069】そして前述したように、前記アクセス対象側は、適正である旨の認証結果が返信されてきたことを条件として当該アクセス希望者のアクセスを許容する。

【0070】図7のS5の現在時刻からなる入力信号、または、図9(B)のS24のIにより、前記アクセス希望者側と前記認証手段側とで共通に変化可能なデータであってアクセス毎に変化可能な共通変数データが構成されている。図7のS5の答えAまたは図9(B)のS25のAにより、前記共通変数データを利用してアクセス毎に内容が変化する可変型パスワードデータが構成されている。前記腕時計33により、前記共通変数データを利用してアクセス毎に内容が変化する可変型パスワードデータを前記アクセス希望者側において生成する可変型パスワードデータ生成手段が構成されている。図8のS7により、前記可変型パスワードデータ生成手段により生成された可変型パスワードデータであってデータ通信により伝送されてきた可変型パスワードデータを受信するデータ受信手段が構成されている。図8のS8～S11により、時間に応じて変化する時間変数データを前記共通変数データとして用いて前記データ受信手段で受信した可変型パスワードデータの適否を判定して認証を行なう時間同期式認証手段が構成されている。図8のS8により、前記データ受信手段により受信された前記可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間(許容値K秒)の範囲内のものである場合には当該誤差に起因したアクセス禁止の認証を行なわない所定誤差許容認証手段が構成されている。図8のS9により、前回のアクセス時から前記誤差許容時間が経過するまでの間において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスしてきた場合に、当該アクセスを許容しない旨の認定を行なうための誤差許容時間内不正アクセス禁止手段が構成されている。図7のS1、S2により、前記の可変型パスワードデータ生成手段のクロック機能の狂いに伴い前記時間変数データに誤差が生

じた場合にそれを自動的に修復させて経時的に誤差が累積されることを防止するための誤差自動修復手段が構成されている。

【0071】前述した図7のS3により、前記可変型パスワードデータ生成手段を所有している本人を確認するための識別データ信号が入力されたことを判別する識別信号入力判別手段が構成されている。そして、この識別信号入力判別手段による入力判別が行なわれたことを条件として前記可変型パスワードデータの生成が可能となる（図7のS3によりYESの判断がなされたことを条件としてS4～S6の処理が可能となる）。また、前述したように、認証手段が前記可変型パスワードデータに基づいたパスワード認証動作を行なう前に、前記アクセス希望者から通知された確認用データであって当該アクセス希望者が予め登録されているものか否かを確認するための登録確認用データ（呼出番号）に基づいて適正である旨の確認結果（呼出番号が前もって登録されている使用許可できるものの番号である旨の確認結果）が得られたことを条件として、前記認証手段が前記パスワード認証動作を実行する。

【発明の効果】本第1発明によれば、アクセス対象が多くなったとしても、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段に認証用データを登録しておくことにより、前記複数のアクセス対象のうちのいずれかにアクセスするべくアクセス希望者が可変型パスワードデータを伝送した場合に、その可変型パスワードデータが前記認証手段に転送されてその認証手段において認証が行なわれるために、多くのアクセス対象毎に認証用データを登録する必要がなくなり、多くのアクセス対象毎に認証データを登録した場合の種々の不都合を極力防止することができる。さらに、時間に応じて変化する時間変数データを共通変化データとして用いて転送されてきた可変型パスワードデータの適否が判定されて認証が行なわれるために、前回のアクセス時と今回のアクセス時とで異なった内容の可変型パスワードデータとなり、セキュリティが向上する。しかも、可変型パスワードデータ生成手段のクロックが狂って時間変数データに誤差が生じた場合にその誤差が自動的に修復されて経時的に誤差が累積されることが防止可能となるために、時間変数データの誤差に起因したアクセス不能状態等が発生する不都合を極力防止することができる。本第2発明によれば、アクセス対象が多くなったとしても、アクセス制御のための認証を統括して行なって集中管理を行なう認証手段に認証用データを登録しておくことにより、前記複数のアクセス対象のうちのいずれかにアクセスするべくアクセス希望者が可変型パスワードデータを伝送した場合に、その可変型パスワードデータが前記認証手段に転送されてその認証手段において認証が行なわれるために、多くのアクセス対象毎に認証用データを登録する必要がなくなり、多くのアクセス対象毎に認証

データを登録した場合の種々の不都合を極力防止することができる。さらに、時間に応じて変化する時間変数データを共通変化データとして用いて転送されてきた可変型パスワードデータの適否が判定されて認証が行なわれるために、前回のアクセス時と今回のアクセス時とで異なった内容の可変型パスワードデータとなり、セキュリティが向上する。さらに、転送されてきた可変型パスワードデータが誤差を有する時間変数データにより生成されたものであっても、当該誤差が予め定められた誤差許容時間内の範囲内のものである場合に、当該誤差に起因したアクセス禁止の認証が行なわれないために、多少の誤差に起因してアクセス不能状態となる等の不都合を極力防止することができる。一方、誤差許容時間を設けた場合に、たとえば可変型パスワードデータが入力途中や伝送途中で盗聴されてその同じ可変型パスワードデータを用いて前記誤差許容時間の範囲内において不正にアクセスしようとする不正行為が発生することが考えられる。すなわち、前記誤差許容時間は、その時間内であれば誤差があってもアクセス禁止の認証を行なわないものであり、誤差許容時間内であれば結果として同じ内容の可変型パスワードデータを複数回受け付けてしまい、この誤差許容時間がセキュリティホールとなってしまふ虞れがある。そこで、本発明によれば、前回のアクセス時から前記誤差許容時間の範囲内において、前回のアクセス時に用いられた可変型パスワードデータと同じ可変型パスワードデータによりアクセスをしてきた場合に、当該アクセスを許容しない旨の認定を行なって誤差許容時間内における不正アクセスを禁止できるようにしたのであり、これによりより一層セキュリティが向上する。

30 【図面の簡単な説明】

【図1】斜視図である。

【図2】フローチャートである。

【図3】作用説明図である。

【図4】作用説明図である。

【図5】作用説明図である。

【図6】斜視図である。

【図7】フローチャートである。

【図8】フローチャートである。

【図9】(A) (B)はそれぞれフローチャートである。

40

【図10】パーソナル端末装置の制御回路図である。

【符号の説明】

3はパーソナル端末装置、2は入力装置、1はキーボード、33は腕時計、13、14はコンピュータ、10は銀行、11はデータバンク、12はコインロッカー、25は発信機である。

【要約】

【課題】 アクセス対象設備が多くなったとしても、パスワードデータの適否を判定するための判定用データをそのアクセス対象設備ごとに登録する必要をなくし、登

50

21

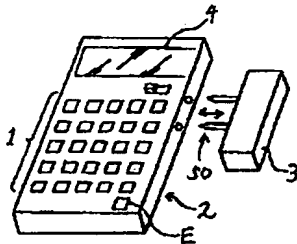
録された判定用データの盗用の危険性を極力抑える。

【解決手段】 アクセス希望者から送られてきたパスワードデータの適否を判定するための判定用データであるシークレット関数 $f(w, x, y, z)$ をコンピュータ 13 または 14 に登録しておき、複数のアクセス対象設備 10, 11, 12 のいずれにアクセスする場合におい

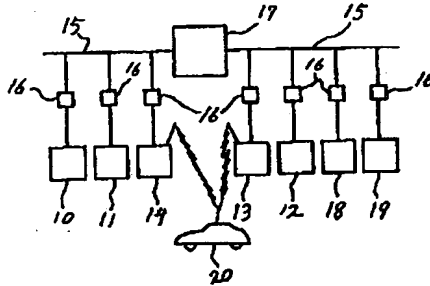
22

てもアクセス対象設備に伝送されてきたパスワードデータをコンピュータ 13 または 14 に転送し、そのコンピュータ 13 または 14 によってパスワードデータの適否を統括して判定して認証を行ない、その認証結果を転送元であるアクセス対象設備に返信するようにした。

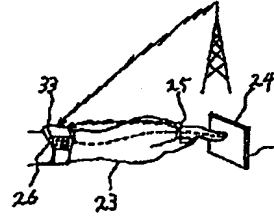
【図 1】



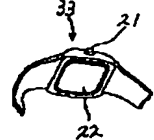
【図 4】



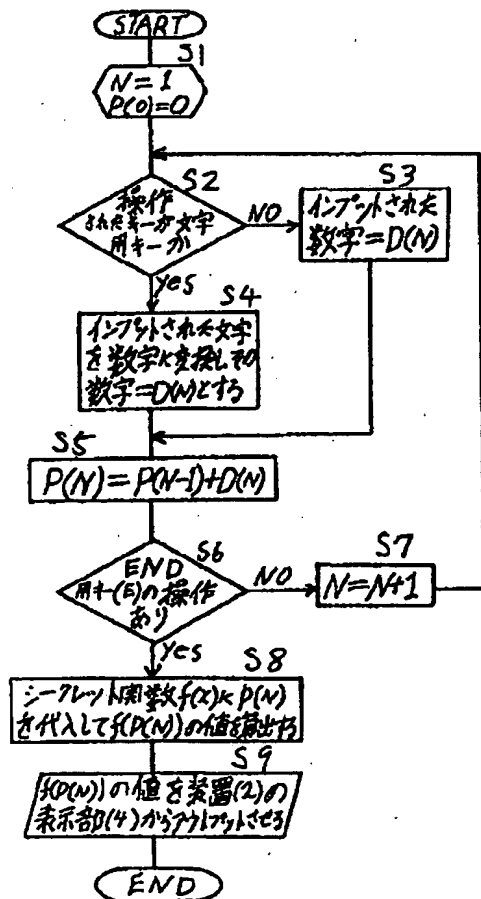
【図 5】



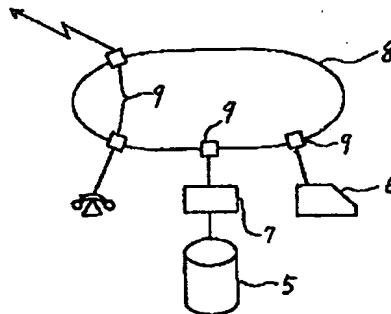
【図 6】



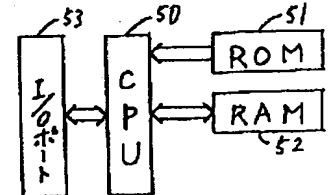
【図 2】



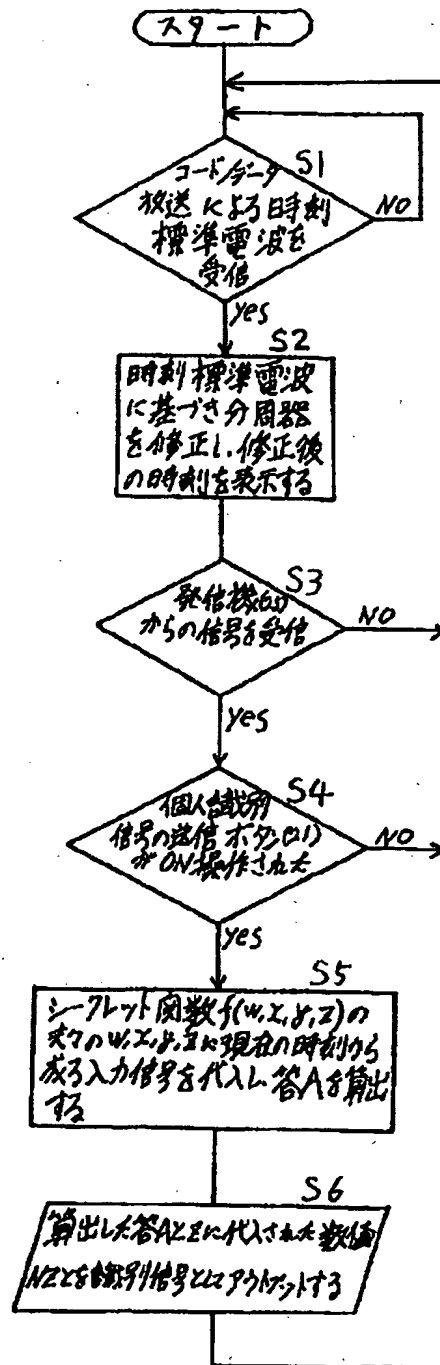
【図 3】



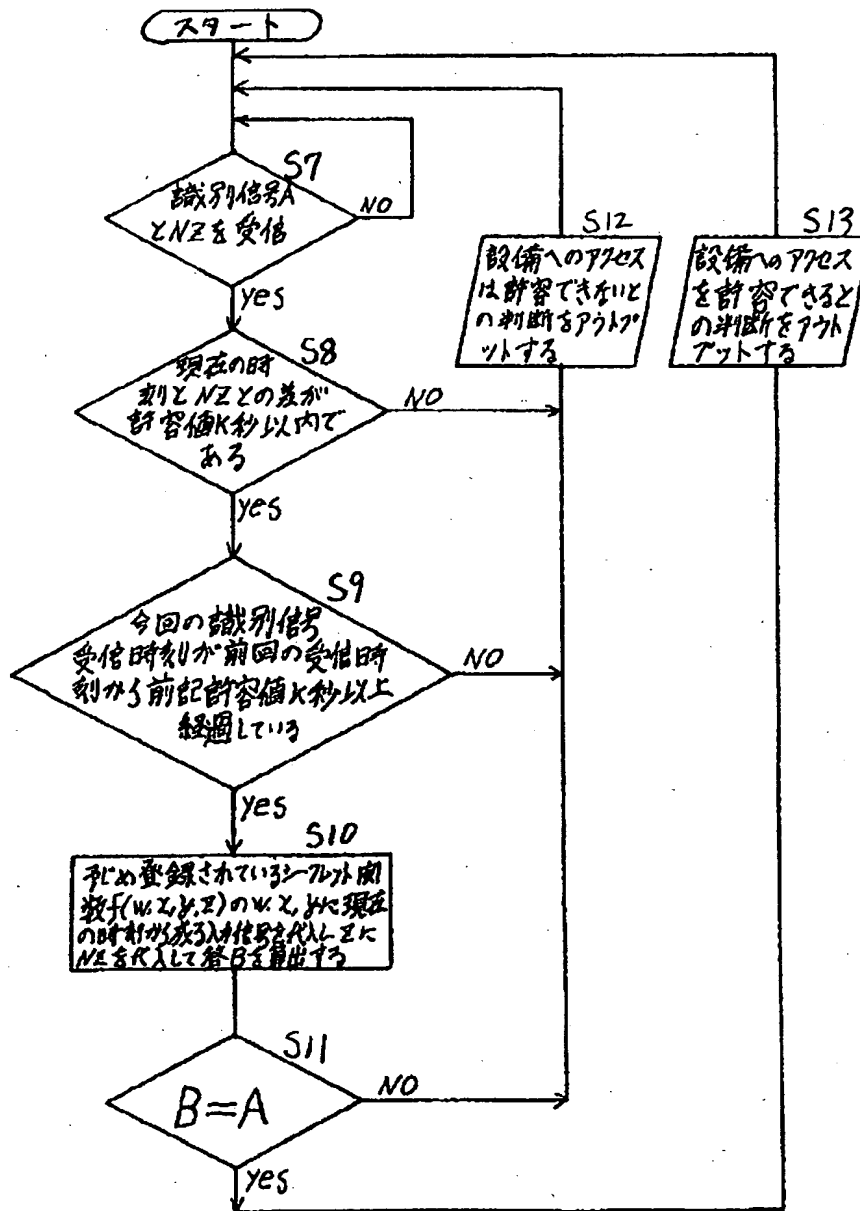
【図 10】



【図7】



【図8】



【図9】

